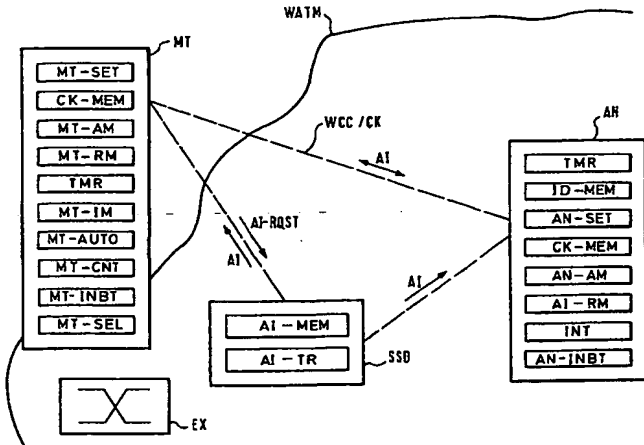




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04Q 11/00	A1	(11) International Publication Number: WO 99/44387 (43) International Publication Date: 2 September 1999 (02.09.99)
(21) International Application Number: PCT/EP99/01251 (22) International Filing Date: 26 February 1999 (26.02.99) (30) Priority Data: 98103449.9 27 February 1998 (27.02.98) EP (71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE). (72) Inventors: KELLER, Ralf; Starenweg 50, D-52146 Würselen (DE). WRONA, Konrad; Ericsson Allee 1, D-52134 Herzogenrath (DE). (74) Agents: VON FISCHERN, Bernhard et al.; Hoffmann . Eitle, Arabellastrasse 4, D-81925 Munich (DE).		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>
(54) Title: AUTHENTICATION METHOD AND AUTHENTICATION DEVICE FOR SECURED COMMUNICATIONS BETWEEN AN ATM MOBILE TERMINAL AND AN ATM ACCESS NODE OF A WIRELESS ATM RADIO COMMUNICATION NETWORK  <p>The diagram illustrates the authentication process. On the left, the Mobile Terminal (MT) contains modules: MT-SET, CK-MEM, MT-AM, MT-RM, TMR, MT-IM, MT-AUTO, MY-CNT, MT-INBT, and MY-SEL. On the right, the Access Node (AN) contains: TMR, ID-MEM, AN-SET, CK-MEM, AN-AM, AI-RM, INT, and AN-INBT. In the center, the Security Server (SSD) contains AI-MEM and AI-TR. A dashed line labeled 'WATM' connects the MT and AN. A solid line labeled 'WCC / CK' connects the MT and AN. A dashed line labeled 'AI' connects the MT to the SSD. A solid line labeled 'AI-RQST' connects the MT to the SSD. A solid line labeled 'AI' connects the SSD to the AN. A solid line labeled 'SSD' connects the SSD to the AN. A box labeled 'EX' is connected to the MT.</p>		
(57) Abstract A mobile terminal (MT) sets up a wireless ATM radio communication connection (WCC) to an access node (AN) of a wireless ATM radio communication network (WATM). On the communication connection (WCC) a secret communication key (CK) is used which has been agreed upon by the ATM access node (AN) and the ATM mobile terminal (MT). Once the operating communication connection (WCC) is established, the mobile terminal (MT) can request authentication information (AI) from the security server (SSD) located in the (WATM) system or another network (FN) connected to the access node (AN). If after setting up the communication connection (WCC) the authentication information (AI) is received in a predetermined time period at said access node (AN), the mobile terminal is authenticated at the access node (AN). Since the communication channel (WCC) is always set up before the authentication procedure, also security functions from other interconnected networks can be accessed and thus a high level of confidentiality as well as security can be maintained.		

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakistan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

5 Authentication Method and Authentication Device for Secured
Communications between an ATM Mobile Terminal and an ATM
Access Node of a Wireless ATM Radio Communication Network.

10

Field of the Invention

The invention relates to a method for setting up a secured
communication between an ATM mobile terminal and an ATM
15 access node of a wireless ATM radio communication network.
Furthermore, the invention relates to an authentication
device for such a wireless ATM radio communication network.
The invention also relates to the ATM access node of such a
wireless ATM radio communication network. Furthermore, the
20 invention relates to an ATM mobile terminal usable within
such a wireless ATM radio communication network.

In wireless ATM radio communication networks, generally two
steps must be performed in order to connect an ATM mobile
25 terminal to an ATM access node, namely an authentication
step where authentication information is exchanged between
the mobile terminal and the access node, and a second step
in which the wireless connection is set up and in which a
secret ciphering key is agreed upon (which is used in an
30 encryption procedure to encrypt the data to be transmitted)
such that the wireless ATM connection has a high degree of
confidentiality. The exchange of authentication information
and the setting up of the wireless connection with the
agreed confidentiality key requires the exchange of signals.
35 between the mobile terminal and the access node according
to a predefined protocol.

5 Some protocols allow the exchange of the shared authentication information prior to setting up the wireless connection with the session key. However, as will be explained below, there are some protocols a session needs to be first established and only then the secret shared
10 authentication information can be made available. This draw-back is very significant, if for example a first signaling protocol is used on the wireless link between the mobile terminal and the access node and another protocol is used between the access node of the ATM communication
15 network and an access node of other interconnected fixed networks.

The invention in particular relates to the establishment of a secure ATM wireless connection between the ATM mobile
20 terminal and the ATM access node for the case where different signaling protocols are used.

Background of the Invention

25 Wireless ATM systems are currently standardized within both the ETSI project BRAN and the ATM Forum Wireless ATM group. Examples of such wireless ATM systems are for example an ATM wireless access communication system (AWACS system), a wireless professional and residential multimedia
30 applications (MEDIAN application) for indoor customer premises networks, the Magic WAND demonstrator (wireless ATM network demonstrator) for indoor and outdoor applications in customer premises and public networks, the SAMBA system, an ATM based mobile system like a broadband
35 mobile communication for multimedia on ATM-basis supported by the German Ministry for Research and Education, or a high performance radio local area network (HIPERLAN system) etc.

5

Each of the aforementioned wireless ATM systems is defined for specific different application areas. Some of them are for example designed for wireless local area networks (LANs) or to the extension or replacement of fixed LANs.

10 Other systems are specifically designed for broadband access (e.g. to UMTS or to the GSM or GPRS core networks) or to point-to-multipoint systems.

A general configuration of interacting networks including
15 wireless ATM systems is shown in the attached Fig. 1a. Such systems are currently investigated in the aforementioned standardizing committees. As is seen in Fig. 1a, several different types of networks are interconnected through access nodes AN (also called access points). The network A
20 may be provided for fixed wireless components communicating through a wireless channel (e.g. through fixed wireless LANs and a network access via microwave links). The network B may comprise mobile end users communicating directly with the fixed network switching elements (e.g. digital cellular
25 telephony, PCS, wireless LAN). The networks C, D may represent mobile switches with fixed end users where the end users have a fixed connection (either wired or wireless) to a switch. The switch and the end user, as a unit, are mobile, with the switch having a wired or
30 wireless connection to fixed network switching elements (e.g. to a fixed network on board of a passenger plane, military aircraft or navel vessel). Furthermore, in the network D mobile switches with mobile end users may be provided, i.e. the mobile terminals establish connections
35 with switches which are themselves mobile and which then establish a connection to a fixed network, as is the case e.g. in LEO satellite based switching to mobile stations, wireless end user devices; wireless connection to mobile switches on emergency or military vehicles). Another

5 example is shown at E, which is summarized as wireless ad
hoc networks. Here, wireless networks are provided, when
there is no access node available (e.g. laptops gathered
together in a business conferencing environment). It also
considers cases where access nodes cannot be placed at
10 arbitrary locations and where plug-and-play and network
flexibility are important considerations (e.g. for a
residential user). This requirement can be met by
supporting auto-configuration of a wireless ATM network.
Both mobile end users and fixed wireless end users are
15 possible. Ad hoc networks can also extend the coverage of
existing access-node-orientated networks by wireless means
by use of forwarding nodes, which act as intermediate relay
points (transfer nodes) and forward ATM packets from one
WATM radio frequency to another WATM radio frequency. It is
20 envisaged that in the initial stage a wireless ATM system
will use an operating frequency of 5 GHz and a available
user data rate of 25 Mbit/s. The estimated cell range will
be between 30 - 50 m indoors and 200 - 300 m outdoors.

25 As shown in Fig. 1a, there are various possibilities how
mobile ATM (asynchronous transmission mode) networks may be
interconnected through the access nodes AN and, since the
communication connections are ATM connections and are
wireless, the security aspect is an important consideration
30 in such a network architecture. In particular, the inter-
operability with security mechanisms of other networks is
an important aspect. Also simplicity of upgrading and
adding new functionalities is very important, especially as
it is impossible to prove that any of the existing
35 practical cryptosystems cannot be broken in future, due to
the progress in mathematical theory and development of new
more efficient algorithms.

5 Therefore, as explained above, several steps have to be performed before a secure ATM connection in the wireless ATM communication network can be guaranteed. This will be explained below with reference to Fig. 1b and Fig. 2.

10 Conventional authentication procedure

Fig. 1b shows a simplified network configuration according to Fig. 1a for explanation purposes. Fig. 1b represents a typical case when the wireless ATM system is a wireless LAN or a broadband access system, where it is desirable that a wireless ATM radio communication network WATM is to be connected to a fixed non-ATM system, for example to an Ethernet via access nodes AN of the WATM system and the FN system. Typically, the Ethernet only supports one secure association establishment protocol.

However, in Fig. 1b the Ethernet is only taken as an example for the non-ATM fixed network and it may be useful to connect a general wireless ATM radio communication network WATM to a network system through access nodes AN, wherein the network system can perform different secure association establishment procedures. Of course, this implies that a signaling gateway is established between the network system and the WATM system.

30 As is also shown in Fig. 1b, a wireless communication connection WCC is set-up between the ATM mobile terminal MT and the ATM access node AN and the ATM signaling is thus terminated in the access node AN. It is generally difficult to design services within the WATM system if these services should rely on functions and services in the fixed networks exactly because the ATM signaling is terminated in the access point AN.

5

With the access node AN clearly being the entry point into the WATM system, it is obvious that the access node AN has to be protected against fraudulent and accidental misuse, such that not any subscriber can have access to the WATM system. As explained before, this is done by a two step mechanism, namely an authentication mechanism where the mobile station MT and the access node AN must recognize each other, and a second step where encryption methods are used on the radio link to provide a confidentiality level on the radio link. Thus, not any arbitrary subscriber station SS, for example from the fixed network SN, should gain an access and should be supported in the WATM system, but only such subscriber stations for mobile stations which are recognized by the WATM system.

20

When a mobile terminal MT desires an access to the WATM system or requires a registration, the following two types of registrations can be distinguished:

- 25 1. The access node AN and the ATM mobile terminal MT must possess a secret authentication information AI and the authentication information must be the same in the access node AN and in the mobile terminal MT. Such an authentication information may typically be an
30 authentication key or a challenge/response information.
2. The ATM mobile terminal MT and the access node AN
"don't know each other"; i.e. they cannot recognize
35 each other.

In both cases, communication keys (encryption/decryption keys) have to be generated and exchanged between the mobile terminal MT and the access node AN in any case. These

5 communication keys CK are used to achieve a confidentially
of the information transmitted on the wireless ATM
connection. Protocols which are used to generate and
exchange such communication keys CK are generally called
"key agreement protocols" and in existing networks like
10 GSM, DECT, IS-54, IS 95 and CDPD, they are combined with
the subscriber authentication, thus building a so-called
"atomic authentication and key agreement (AKA) protocol".

Generally, there are two categories of AKA protocols that
15 can be used for setting up the communication between the
ATM mobile terminal MT and the ATM access node AN. Namely,
the first category comprises for example the usage of the
Diffie-Hellman encrypted key exchange (DH-EKE) protocol or
the simple key exponential key exchange (SPEKE) protocol
20 (see e.g. reference [1]: B. Schneier, "Applied
Cryptography, Second Edition, Wiley, 1992" and reference
[2]: D. Jablon "Strong Password only Authenticated Key
Exchange, ACM Computer Communication Review, October
1996"). A typical flow chart of how a secured communication
25 between ATM mobile terminal MT and an ATM access node AN of
a wireless ATM radio communication network WATM using this
kind of protocol is achieved, is illustrated in Fig. 2.

In Fig. 2, the mobile terminal MT and the access node AN
30 exchange authentication information in step ST2 after
starting the setup procedure in step ST1. In ST3 it is
checked whether the mobile terminal MT and the access point
AP recognize each other, i.e. whether the access node AN
have stored an authentication information which coincides
35 with that sent by the mobile terminal MT. If this is not
so, "N" in step ST3, the exchange of authentication
information is repeated in step ST2. If the mobile terminal
MT and the access point AM use the same authentication
information, "Y" in step ST3, then the MT and the access

5 node AN agree on a secrete ciphering key in step ST4 (using the AKA protocol). If MT/AN have agreed on a secret session key (communication or ciphering key) in step ST4, then a secure wireless ATM communication connection WCC has been established and the usual communication signaling protocol
10 for information transfer can be setup in step ST5. The setup procedure comes to an end in step ST6.

Therefore, using the conventional Diffie or Diffie-Hellman encrypted key exchange (DH-EKE) or the simple key ex-
15 ponential key exchange (SPEKE) protocol, the authentication information AI is in fact established before completing the AKA protocol. However, there is a second category of AKA protocols, where the secret shared authentication information is not available before setting up the wireless
20 communication connection WCC based on the agreed session encryption keys. That is, using protocols of the second category means that the shared authentication information only becomes available after, the secured communication connection has been set up.

25

As is illustrated in Fig. 1b, the situation becomes even more difficult if different signaling protocols are used on the wireless ATM communication connection WCC between the mobile terminal MT and the access node AN (i.e. an WATM
30 signaling) and between the access node AN of the WATM network and the access nodes AN of the fixed networks SN, for example an internet signaling or an UMTS signaling. That is, if the access of the AN of the WATM communication network should be flexible enough to interconnect to
35 different signaling protocols (for example internet signaling or UMTS signaling) then different authentication procedures or different AKA protocols may have to be used dependent on the used protocol between the ATM system and the fixed network FN. Therefore, sometimes the category 1

5 AKA protocol may have to be used and some times the category 2 AKA protocol may have to be used. Thus, in some cases the authentication information may not be available before setting up the encrypted ATM wireless communication connection WCC.

10

Summary of the Invention

As described above, the problem with setting up ATM wireless communication connections between a ATM mobile terminal and a ATM access node essentially resides in the fact, that either different kinds of AKA protocols are to be set up to the access node or that in fact the authentication information is not available prior to completing the AKA protocol.

20

Therefore, the object of the present invention is to provide a method, an authentication device, an ATM access node, an ATM mobile terminal as well as a ATM communication system, in which a secure communication between a ATM mobile terminal and an ATM access node can be established.

A secure communication is preferably to be established even if the authentication information is not available when completing the protocol or if various different AKA protocols are to be used on the access node or if security mechanisms of other interconnected networks are to be used.

30

Solution of the Object

35 Essentially this object is solved by a method for setting up a secured communication between an ATM mobile terminal and an ATM access node of a wireless ATM radio communication network, comprising the step of setting up a wireless ATM radio communication connection between said

10

5 ATM mobile terminal and said ATM access node without performing an authentication information checking procedure
therebefore, wherein an information exchange on said
wireless ATM radio communication connection is performed
by using a secret communication key agreed upon by said ATM
10 access node and said ATM mobile terminal.

Furthermore, this object is solved by an authentication device, in particular for a wireless ATM radio communication network, comprising, an authentication
15 information storage means for storing a plurality of authentication informations each corresponding to a respective ATM mobile terminal served by a wireless ATM radio communication network, and an authentication information transmisssion means for issuing an
20 authentication information in reponse to receiving an authentication information request from an ATM mobile terminal after a ATM wireless radio communication connection has been setup between said requesting ATM mobile terminal and said ATM access node using a secret
25 communication key agreed upon by said ATM access node and said ATM mobile terminal.

The object is also solved by an ATM access node of a wireless ATM communication network for setting up a secured
30 wireless ATM communication connection to an ATM mobile terminal, said ATM access node comprising, a setup means for setting up a wireless ATM radio communication connection to said ATM mobile terminal without performing an authentication information checking procedure
35 therebefore, a secret communication key storage means for storing a secret communication key used by said ATM mobile terminal and said ATM access node for performing wireless ATM communications.

5 Furthermore, the object is solved by an ATM mobile terminal for setting up a secured communication to an ATM access node of a wireless ATM communication network, comprising, a setup means for setting up a wireless ATM radio communication connection to said ATM access node without
10 performing an authentication information checking procedure therefore, a secret communication key storage means for storing a secret communication key used by said ATM mobile terminal and said ATM access node for performing wireless ATM communications.

15

Finally, the object is also solved by an ATM wireless communication network according to claim 32.

The basic idea of the invention is to provide user chosen
20 confidentiality level on the radio link by means of setting up a secure association between the WATM access node and the wireless ATM mobile terminal without using an authentication as a first step. That is, according to the invention, a wireless ATM radio communication connection is
25 established by agreeing upon a secret communication key CK between the ATM access node and the ATM mobile terminal, wherein no authentication information checking procedure is performed therefore.

30 Another aspect of the invention is that once the secured wireless ATM radio communication connection has been established between the mobile terminal and the access node, the mobile terminal tries to get the secret shared authentication information by use of higher level protocols
35 communication from an authentication device provided in the wireless ATM communication network or provided in a network which is connected to the access node (with which the mobile terminal has setup the secure ciphered communication link) through a signalling path. This authentication device

5 comprises an authentication information search means for
storing a plurality of authentication informations each
corresponding to a respective ATM mobile terminal served by
said wireless ATM radio communication network. When the ATM
communication connection has been set up, the mobile
10 terminal requests an authentication information from this
authentication device and only then an authentication
procedure is performed at the access node with the
authentication information being provided by the
authentication device.

15

Another aspect of the invention is that the mobile terminal
must receive the secret shared authentication information
from the authentication device within a predefined period
or within a period which has been negotiated between the
20 mobile terminal and the access node. If the mobile terminal
receives the secret shared authentication information
within this period, then it either authenticates itself at
the access node or this task is being taken care of by the
authentication device which initially provided the
25 authentication information.

If the time runs out, i.e. if the mobile terminal cannot
authenticate itself at the access node within the
predefined time period, then the already setup wireless ATM
30 radio communication connection is interrupted (closed) and
information regarding the mobile terminal (which has
unsuccessfully attempted an authentication) is stored in
the access node. Preferably, if the same mobile terminal
has already failed an authentication a predetermined number
35 of times, then further access requests from this mobile
terminal are immediately rejected by the access node.

Preferably, before the authentication procedure is
performed at the access node, the mobile terminal (the

5 user) can choose a predetermined communication key
(confidentiality level) to be used on the wireless ATM
communication connection. Thus, the user or the user
application itself can choose the degree of confidentiality
which it desires on the wireless communication connection.

10

If the authentication device is located or part of the WATM
system a signalling path is established through the access
node to the authentication device in order to request the
authentication information. This information is then
15 preferably transferred back to the mobile terminal through
the already setup ciphered communication link.

If the authentication device is located or part of another
network connected to the access node via a communication
20 link, depending on the type of WATM network and the type of
the connected network, a signalling path is setup to the
authentication device through the access node to request
the authentication information. Preferably, this
authentication information is again transferred back to the
25 mobile terminal along the already setup communication
(ciphered) channel.

Further advantageous embodiments and improvements of the
invention may be taken from the dependent claims.
30 Hereinafter, the invention will be described with reference
to its advantageous embodiments and the attached drawings.

5 Brief Description of the Drawings

In the drawings:

Fig. 1a shows a principle overview of possible network
10 configurations including a wireless ATM network;

Fig. 1b shows an example where a wireless ATM system WATM
is connected to a fixed network FN through access
nodes AN;

15

Fig. 2 shows a conventional method to setup a secured
communication between ATM mobile terminal and an
ATM access node;

20 Fig. 3 shows an authentication device SSD, an access
node AN and a mobile terminal MT according to the
invention;

25 Fig. 4 shows a principle flowchart of the method
according to the invention;

Fig. 5 shows a more detailed flowchart of setting up a
secured communication according to the invention.

30 Principle of the Invention

As explained before, one of the big disadvantages of the
existing secret-based AKA protocols is that the shared
authentication information has to be established between
35 the mobile terminal MT and the access node AN prior to
completing the protocol. However, when different signaling
protocols are used on the wireless link between the mobile
terminal MT and the access node AN (WATM signaling) and
between the access node AN and other fixed network nodes,

15

5 (e.g. internet signaling) then the setup of shared secret knowledge prior to secure association might be extremely difficult. This happens also when the access node AN is not connected to a fixed ATN network. In such case, some protocols might be used (e.g. Diffie-Hellman) to build out
10 a temporary security association between AN and NT, i.e. to setup shared secret keys for radio link encryption. After setting a secure channel a regular end-to-end authentication might be done.

15 According to the invention a method is established that provides a user chosen confidentiality level on the radio link by means of setting up a secure association between the WATM access point and the wireless ATM terminal without any authentication in the first run. After the secure
20 association has been established, for example using an unauthenticated variant of the conventional protocol, the mobile terminal MT tries to get the secret shared authentication information by communicating with an authentication device (also called a security server) in
25 the WATM network (or in fact in an interconnected fixed network) through a communication (signalling) channel setup means of a higher level protocol. The transfer of the authentication information then takes place along the already setup ciphered communication channel.

30

If the mobile terminal gets to secret shared authentication information within a predefined or negotiated period, it performs an authentication itself at the access node AN. This authentication procedure can be accomplished using
35 either an authenticated variant of the flexible AKA protocol or other mechanisms. Otherwise, the respective timer in the access node AN runs out and the access AN closes to wireless connected to the mobile terminal MT. Attacks of fraudulent or accidental misuse can be prevented

5 to some extent by storing the MAC address or other suitable information about the mobile terminal MT within the access point AN. After N unsuccessful connection setups further access requests from this mobile terminal MT are immediately rejected by the access node AN.

10

Therefore, whilst all AKA protocols in the prior art use an authentication procedure before setting up the actual wireless ATM communication connection, one of the basic principles of the invention is based on the idea to first
15 setup the wireless ATM communication between the mobile terminal MT and the access node AN by selecting and agreeing upon a common encryption communication key and only thereafter possibly an authentication is performed.

20 Embodiments of the mobile terminal MT, access node AN and the authentication device of the WATM system performing such a function are described below with reference to Fig. 3. It should be understood that Fig. 3 in principle corresponds to Fig. 1b, i.e. a plurality of mobile
25 terminals MT are connected to a wireless ATM system and a wireless secured ATM communication connection WCC is to be set up between the mobile terminals MT and the access node AN.

30 Embodiment of the mobile terminal MT/Access node AN

Hereinafter, the functions performed by the mobile terminal MT and the access node AN according to the invention as shown in Fig. 3 will be illustrated with reference to the
35 communication connection setup method as shown in Fig. 4.

In Fig. 3 the ATM mobile terminal MT comprises a setup means MT-SET for setting up a wireless ATM radio communication connection WCC to said ATM access node AN.

5 Likewise, the access AN comprises a setup means AN-SET for setting up the wireless ATM radio communication connection WCC to said ATM mobile terminal MT. In the mobile terminal MT and the access node AN a respective secret communication key KC storage means CK-MEM stores a secret communication
10 key CK used by said ATM mobile terminal MT and said ATM access node AL for performing wireless ATM communications. After starting the setup procedure in step S1 in Fig. 4, the setup means MT-SET of the mobile terminal MT sends a setup request to the access node AN by means of a protocol,
15 to setup a secure association, i.e. a secured wireless ATM radio communication connection WCC to said setup means AN-SET of the access node AN. As is seen in Fig. 4, there is no authentication procedure before or after the setting up procedure in S2. That is, in step S2 a fully operable (i.e.
20 usable for data transfer) and ciphered wireless ATM radio communication link is setup which uses a secret communication key CK, (i.e. a confidentiality level or encryption key) which has been agreed upon by said ATM mobile terminal MT and said ATM access node AN for
25 performing wireless ATM communications.

In step S2, a secrete key selection means MT-SEL of said mobile terminal MT can preferably predefine or select one of a plurality of secret communication keys CK stored in
30 the secret communication key storage means CK-MEM within the mobile terminal MT. That is, in step S2, the user or the user application can predefine a desired confidentiality level on the wireless ATM radio communication connection WCC.

35

First, in step S2 a user chosen confidentiality level can preferably be provided on the radio link by means of setting up a secure association between the WATM access node AN and the wireless ATM mobile terminal without an

5 authentication in the first run. Thus, by contrast to the category 1 AKA protocols, the protocol illustrated in fig. 4 does not require the setup of shared authentication information between the mobile terminal MT and the access node AN prior to completion of the protocol. The procedure
10 is also applicable to category 2 protocols, because there is yet again no necessity to setup the secret shared authentication information before setting up the security association (i.e. the encryption key). Thus, the procedure in Fig. 4 is intrinsically different to what was described
15 above for the category 1, category 2 setup protocols, since an authentication information agreement is not necessary before setting up of the operable wireless ATM radio communication connection WCC.

20 After step S2 immediately the real communication protocol for information transfer between MT/AN can be set up in step S6 whereafter the setup procedure comes to an end in step S7.

25 Inclusion of the Authentication Information

Whilst there is no necessity to perform an authentication before the setup of the communication channel WCC in Fig. 3, 4, preferably such an authentication procedure may be
30 carried out after step S2, as is shown in more detail in the flow chart in Fig. 5.

To realize this authentication procedure, the wireless ATM network WATM (or any interconnected non-ATM or ATM fixed
35 network) preferably comprises an authentication device SSD comprising an authentication information storage AI-MEM for storing a plurality of authentication informations AI each corresponding to a respective ATM mobile terminal MT served by said wireless ATM radio communication network WATM.

5 Furthermore, the device SSD comprises an authentication
information transmission means TR for issuing an
authentication information AI in response to receiving an
authentication information request AI-RQST from an ATM
mobile terminal MT after said ATM wireless radio
10 communication connection WCC has been setup between the ATM
mobile terminal MT and said ATM access node AN.

Instead of just exchanging authentication information
between MT and AN, an authentication means MT-AN of the
15 mobile terminal MT requests an authentication information
from the authentication device SSD (hereinafter also called
a security server) of the WATM network (or the
interconnected fixed network FN) through higher layer
protocols in step S3. This request message is denoted AI-
20 RQST in Fig. 3. In response to said request message AI-
RQST, the security server SSD reads out from the memory AI-
MEM an authentication information corresponding to the
mobile terminal MT requesting such information. If the
requesting mobile terminal MT is an admitted (subscribed)
25 mobile terminal MT, then the security server SSD should
have an entry for this mobile terminal MT in the memory AI-
MEM.

In response to such a request AI-RQST the mobile terminal
30 MT is authenticated at the access node AN. This can take
place either by the security server SSD transferring the
requested authentication information AI directly to the
access node AN or alternatively the security server SSD
returns the authentication information AI to the mobile
35 terminal MT via the already established secured (ciphered)
communication channel WCC. At the mobile terminal the
authentication information AI is received in an
authentication information reception means MT-RM.

20

5 Having established the secured communication connection WCC
between the mobile terminal MT and the access node AN
authentication information AI provided by an authentication
device SSD located within the WATM system or even an
interconnected network can now be transferred back to the
10 mobile terminal MT in a secured or ciphered manner through
the communication connection WCC.

Then the mobile terminal MT itself performs the
authentication procedure with the access node AN by
15 transferring the received authentication information AI to
the access node AN. In both scenarios, the ATM mobile
terminal MT is authenticated at the ATM access node by
means of the transfer of the authentication information AI
which identifies the ATM mobile terminal MT at the ATM
20 access node AN. Therefore, if an authentication information
reception means AI-RM in the access node AN receives an
authentication information AI, an authentication means AN-
RN in said ATM access node AN performs the authentication
of the ATM mobile terminal MT when the received
25 authentication information AI is one that identifies the
requesting ATM mobile terminal MT as an admitted ATM mobile
terminal MT.

Therefore, no matter where to the authentication
30 information transmission means AI-TR of the security server
SSD transmits the authentication information AI, an
authentication procedure can always be performed
successfully in step S5 if the authentication information
AI is one that is recognized by said access node AN. That
35 is, an authentication means MT-AN of said ATM mobile
terminal can send an authentication information request
message AI-RQST in step S3 in Fig. 5 to the network
authentication device SSD and an authentication information
reception means MT-RM receives that authentication

5 information AI from said network authentication device SSD in response to the request message. Alternatively, the access node authentication means AN-AM performs the authentication on the basis of authentication information received from the security server directly.

10

Preferably, after the access node AN has finalized the setup of the wireless communication connection WCC to said mobile terminal MT, a timer TMR in said access node AN can be set in step S2 in Fig. 5. Preferably, the timer TMR in
15 AN sets a predetermined time period in which an authentication information reception by AI-RM in AN is expected. Therefore, independently as to whether the authentication information AI is transmitted by the security server SSD or the mobile terminal MT itself, in
20 step S4 a determination is made by the timer TMR in AN as to whether or not the authentic information AI has been received in a predetermined time period. If it has been received, "Y" in step S4 in Fig. 5, then the normal authentication procedure can be performed in step S5. If
25 "N" in step S4, then the timer TMR in AN waiting for the input of the authentication information from MT (directly or through SSD) runs out. In this case, the previously setup wireless ATM communication connection WCC is closed in step S8 by an interrupt means INT in AN .

30

Preferably, an identity memory ID-MEM stores an identity information II, MAC of the ATM mobile terminal MT whose communication connection WCC has been released (closed). The identity information can for example be the MAC address
35 of the requesting mobile terminal MT (MAC: Mobile Access Code) .

Furthermore, if the access node AN recognizes that the mobile terminal MT presently requesting an authentication

- 5 has already previously been trying to setup a communication to the access node AN, also the number of retries MTr can be compared with a maximum number of retries N in step S10. If the same mobile terminal MT has requested an authentication more than N times, then an access node
- 10 inhibition means AN-INBT will completely inhibit or reject any further setup requests from this mobile terminal MT in step S11, whereafter the procedure comes to an end in step S12.
- 15 The interrupt means INT in the ATM access node AN is responsible for closing an already set up secure wireless radio communication WCC, if said authentication information reception means AI-RM does not receive the authentication information from MT within the predetermined time period as
- 20 is determined by the timer TRM in AN. If "N" in step S10, the procedure goes back to step S2 to allow the setup of a communication connection WCC again in step S2.

Preferably, also the ATM mobile terminal MT comprises a

25 timer TMR and if after said sending of said authentication information request message AI-RQST an authentication information AI is not received from said network authentication device or security server SSD within a predetermined period, an interrupt means MT-IM of said ATM

30 mobile terminal MT will close the setup wireless ATM radio communication networks WCC itself. The reason is, that at this point it can hardly be expected that the security service SSD of the WATM system will return an authentication information AI, i.e. that it is hardly

35 likely that the mobile terminal MT has really a valid subscription for setting up communication connections in the WATM communication system.

5 Preferably, the ATM mobile terminal MT also comprises an automatic repetition means MT AUTO for automatically repeating a setup attempt after a predetermined time interval. That is, even before the security server SSD returns a negative response, i.e. that no authentication
10 information can be found in the memory AI-MEM for the presently calling mobile calling MT, the mobile terminal MT can automatically again request the setup of a communication connection WCC to said access node AN.

15 If the mobile terminal MT has performed a predetermined number of repetitive setup requests, as counted by a counter MT-CNT, then an inhibition means MT-INHB of the mobile terminal MT inhibits any further setup requests after a predetermined number N of attempts.

20 Therefore, not only the access node AN can reject further setup requests by the same mobile terminal MT but also the mobile terminal MT itself may decide and recognize that in fact the security server SSD has no information stored
25 whatsoever that would indicate that the presently calling mobile terminal MT is one that has been registered for wireless ATM connections to said access node AN.

Therefore, the above novel protocol can be summarized as
30 follows (see also Fig. 5):

S2: Setup a secure association (a secured communication connection WCC) between the mobile terminal MT and the access node AN without any
35 authentication procedure; start a timer TMR in the access node;

S3/S4: If the mobile terminal MT gets secret shared authentication within the predetermined time

5 period through the ciphered communication channel
WCC then the authentication takes place. If not,
the access node interrupt means INT interrupts or
closes the already setup communication connection
WCC in step S8.

10

S5: Either the mobile terminal MT authenticates
itself at the access node AN or the security
server authentication device SSD authenticates
the mobile terminal at the access node AN. If
15 there is no time out by the timer TMR in the
access node AN or the timer TMR in the mobile
terminal MT, the general communication protocol
for information transfer is set up between MT and
AN in step S6.

20

Industrial Applicability

As explained above a secure setup of a communication
connection between MT and AN is established even if no
25 authentication can be performed in the first run as
explained with reference to Fig. 4. Authentication is
performed afterwards either between MT and AN or between
the authentication device SSD and AN. This is useful for
example in a wireless ATM mobile terminal without hardware
30 support for storing authentication information (e.g. a SIM
card).

By the provision of the communication key memory CK-MEM,
the operator of the mobile terminal MT or in fact the user
35 application itself can establish a user-chosen
confidentiality level without following authentication,
e.g. to allow access of mobile terminals MT to networks in
semi-public areas (e.g. airports). First, for example a
user-application like a program running on a LAPTOP can -

5 without a hardware support for storing authentication
information like a SIM card - request an authentication
information from a security server SSD and if a
registration of such an authentication information has been
previously performed in the memory AI-MEM of the security
10 server SSD, than an access of the mobile terminal MT to the
network is granted.

Furthermore, it should be noted that the authentication
device SSD does not necessarily have to be a part of the
15 WATM system. It can also be a part of the interconnected
ATM fixed network which is shown in Fig. 2. However,
confidentiality of user data on the ATM wireless radio
connection WCC can be guaranteed, even if the fixed network
is only involved after the setup of the security
20 association, for example if the authentication information
is requested from a security server SSD of the fixed
network and is then - in a secure ciphered manner -
transferred back to the mobile terminal through the secured
communication channel.

25

Thus, a security service SSD for WATM systems can be
implemented, that can be used in a non-ATM fixed network
environment, i.e. if ATM calls are only used on the
wireless radio link in the WATM system, whilst an ordinary
30 digital transmission is used in the fixed network. Again,
since the confidentiality is ensured on the wireless
communication connection WCC, the authentication
information can be requested and supplied by any security
server SSD which is located even in the fixed network
35 environment. This means that the transfer of the
authentication information takes place along a wireless ATM
communication connection which is already secured by the
agreed selected secret ciphering key CR.

5 However, the inventive method, authentication device,
mobile terminal and the access node can also be used in
cases, where an ATM based fixed network implements security
services on top of the ATM layer. This means, if the fixed
network system is also an ATM-based fixed network, first
10 the communication channel WCC with its confidentiality
level is setup between the mobile terminal MT and the
access node AN of the wireless ATM system (or in fact to an
access node AN of the ATM-based fixed network) and
thereafter the (secured) authentication information
15 exchange is performed. For requesting and receiving the
authentication information from a security server SSD of
the ATM-based fixed network, a separate signaling channel
from the access node AN of the WATM system to the access
node AN of the ATM-based fixed network is preferably used.

20 The present invention provides confidentiality in different
wireless ATM systems which are adapted for private and/or
business and/or public environments or even mixed
environments. Since the communication channel WCC is setup
25 before a possible authentication procedure, there is
provided the major advantage that security mechanisms
within the WATM system or even security mechanisms from
possibly interconnected fixed networks (non-ATM or ATM) can
be accessed through the secured link WCC or can even be
30 combined, in order to build a security architecture that
offers much higher security level. Since the mobile
terminal MT has access to the security functions located
elsewhere in an interconnected network, a security
architecture can be built, which is more flexible and which
35 can offer a much higher security level.

Whilst the invention has been described with reference to
its embodiments and the drawings to illustrate what is
currently considered as the best mode of the invention, it

5 is clear, that various modifications and variations will be possible for those skilled in the art in view of the above technical teachings. Therefore, the invention is not restricted to the present description and the scope of the invention is defined by the attached claims. In these
10 claims, reference numerals only serve clarification purposes and to not limit the scope of the invention. In the drawings the same or similar reference numerals designate the same or similar parts or steps.

Claims

- 10 1. A method for setting up a secured communication
between an ATM mobile terminal (MT) and an ATM access
node (AN) of a wireless ATM radio communication
network (WATM), comprising the step of setting up (S2)
a wireless ATM radio communication connection (WCC)
15 between said ATM mobile terminal (MT) and said ATM
access node (AN) without performing (ST2, ST3) an
authentication information checking procedure
therebefore, wherein an information exchange on said
wireless ATM radio communication connection (WCC) is
20 performed by using a secret communication key (CK)
agreed upon by said ATM access node (AN) and said ATM
mobile terminal (MT).
2. A method according to claim 1,
25 *characterized in that*
after said setting up of said wireless ATM radio
communication connection (WCC) between said ATM mobile
terminal (MT) and said ATM access node (AN) is
completed (S2), said ATM mobile terminal (MT) is
30 authenticated (S3, S5; S4, S8) at said ATM access node
(AN) by transferring authentication information (AI)
identifying said ATM mobile terminal (MT) to said ATM
access node (AN).
- 35 3. A method according to claim 2,
characterized in that
said ATM mobile terminal (MT) sends an authentication
information request message (AI-RQST, S3) to a network

5 authentication device (SSD) provided by said wireless
ATM communication network (WATM) or by a further
interconnected network (FN).

4. A method according to claim 3,

10 *characterized in that*

said authentication information (AI) is transferred
(S4) to said ATM mobile terminal (MT) in response to
said request message (AI-RQST) and said ATM mobile
terminal (MT) performs an authentication procedure at
15 said ATM access node (AN) using said transferred
authentication information (AI).

5. A method according to claim 3,

characterized in that

20 in response to said request message (AI-RQST), said
network authentication device (SSD) of said wireless
ATM communication network (WATM) performs (S5) an
authentication procedure for said ATM mobile terminal
(MT) at said ATM access node (AN) using said requested
25 authentication information (AI).

6. A method according to claim 2,

characterized in that

after said secure wireless ATM radio communication
30 connection (WCC) has been set up (S2), a timer (TMR)
in said ATM access node (AN) is started and said
already setup wireless ATM radio communication
connection (WCC) is closed by said ATM access node
(AN) if said ATM access node (AN) does not receive an
35 authentication information (AI) for said ATM mobile
terminal (MT) within a predetermined time period (S8).

5 7. A method according to claim 6,

characterized in that

identity information (II, MAC)) of said ATM mobile
terminal (MT) and the number of authentication retries
(MTr) is stored (ID-MEM) in said ATM access node (AN)

10 if said ATM access node (AN) does not receive said
authentication information (AI) within said
predetermined time period (S9).

8. A method according to claim 7,

15 *characterized in that*

when said number of authentication retries (MTr)
exceeds (S10) a predetermined number (N), further
requests by said ATM mobile terminal (MT) to set up a
wireless ATM radio communication connection (WCC)

20 between said ATM mobile terminal (MT) and said ATM
access node (AN) are rejected (S11) by said ATM access
node (AN).

9. A method according to claim 1,

25 *characterized in that*

said secret communication key (CK) is selected by said
ATM mobile terminal (MT) during the setting up of the
wireless ATM radio communication connection (WCC).

30 10. A method according to claim 1,

characterized in that

to said wireless ATM radio communication network
(WATM) access node (AN) is connected a non-ATM fixed
network (FN) providing functions and services to a

35 plurality of fixed network subscribers (SS), wherein
said ATM mobile terminal (MT) accesses said functions
and services via said secured wireless ATM radio

5 communication connection setup between said ATM mobile terminal (MT) and said ATM access node (AN).

11. An authentication device (SSD), in particular for a wireless ATM radio communication network (WATM),
10 comprising:

a) an authentication information storage means (AI-MEM) for storing a plurality of authentication informations (AI) each corresponding to a
15 respective ATM mobile terminal (MT) served by a wireless ATM radio communication network (WATM); and

b) an authentication information transmisssion means (TR) for issuing an authentication information (AI) in reponse to receiving an authentication information request (AI-RQST) from an ATM mobile terminal (MT) after a ATM wireless radio communication connection (WCC) has been setup
20 between said requesting ATM mobile terminal (MT) and said ATM access node (AN) using a secret communication key (CK) agreed upon by said ATM access node (AN) and said ATM mobile terminal (MT).
25

30

12. A device according to claim 11,

characterized in that

said transmission means (AI-TR) is adapted to transfer said authentication information (AI) back to said
35 requesting ATM mobile terminal (MT).

5 13. A device according to claim 11,
characterized in that
said transmission means (AI-TR) is adapted to transfer
said authentication information (AI) to said ATM
access node (AN) to perform an authentication
10 procedure for said ATM mobile terminal at said ATM
access node (AN).

14. A device according to claim 11,
characterized in that
15 to said wireless ATM radio communication network
(WATM) access node (AN) is connected a non-ATM fixed
network (FN) providing functions and services to a
plurality of fixed network subscribers (SS), wherein
said ATM mobile terminal (MT) access said functions
20 and services via said secured wireless ATM radio
communication link setup between said ATM mobile
terminal and said ATM access node (AN).

15. An ATM access node (AN) of a wireless ATM
25 communication network (WATM) for setting up a secured
wireless ATM communication connection (WCC) to an ATM
mobile terminal (MT), said ATM access node (AN)
comprising:

30 a) a setup means (AN-SET) for setting up (S2) a
wireless ATM radio communication connection (WCC)
to said ATM mobile terminal (MT) without
performing (ST2, ST3) an authentication
information checking procedure therebefore;

35 b) a secret communication key (CK) storage means
(CK-MEM) for storing a secret communication key
(CK) used by said ATM mobile terminal (MT) and

5 said ATM access node (AN) for performing wireless
 ATM communications.

16. An ATM access node (AN) according to claim 15,
 characterized by
10 an authentication means (AN-AM) for authenticating
 said ATM mobile terminal (MT) at said access node (AN)
 when an authentication information reception means
 (AI-RM) receives authentication information (AI)
 identifying said ATM mobile terminal (MT).

15
17. An ATM access node (AN) according to claim 16,
 characterized in that
 said authentication information reception means (AI-
 RM) receives said authentication information (AI) from
20 said ATM mobile terminal (MT).

18. An ATM access node (AN) according to claim 16,
 characterized in that
 said authentication information reception means (AI-
25 RM) receives said authentication information (AI) from
 a network authentication device (SSD) separately
 provided by said wireless ATM radio communication
 network (WATM) or by a further or interconnected
 network (FN).

30
19. An ATM access node (AN) according to claim 16,
 characterized in that
 said ATM access node (AN) comprises a timer (TMR),
 which is started after said wireless ATM communication
35 connection (WCC) between said access node (AN) and
 said ATM mobile terminal (MT) has been setup by said
 setup means (AN-SET).

- 5 20. An ATM access node (AN) according to claim 19,
 characterized in that
 said ATM access node (AN) comprises an interrupt means
 (INT) for closing an already setup secured wireless
 radio communication connection (WCC) if said
10 authentication information reception means (AI-RM)
 does not receive an authentication information for
 said ATM mobile terminal (MT) within a predetermined
 time period (S8) as determined by said timer (TMR).
- 15 21. An ATM access node (AN) according to claim 20,
 characterized in that
 identity information (II, MAC)) of said ATM mobile
 terminal (MT) and the number of authentication retries
 (MTr) is stored in an identity memory (ID-MEM) in said
20 ATM access node (AN) if said authentication
 information reception means (AI-RM) does not receive
 said authentication information (AI) within said
 predetermined time period (S9).
- 25 22. An ATM access node (AN) according to claim 21,
 characterized in that
 when said number of authentication retries (MTr)
 exceeds (S10) a predetermined number (N), an
 inhibiting means (AN-INBT) of said ATM access node
30 (AN) inhibits further requests by said ATM mobile
 terminal (MT) to set up a wireless ATM radio
 communication connection (WCC) between said ATM mobile
 terminal (MT) and said ATM access node (AN).
- 35 23. An ATM access node (AN) according to claim 15,
 characterized in that
 to said ATM access node (AN) is connected a non-ATM
 fixed network (FN) providing functions and services to

35

5 a plurality of fixed network subscribers (SS), wherein
said ATM mobile terminal (MT) accesses said functions
and services via said wireless ATM radio communication
link setup between said ATM mobile terminal and said
ATM access node (AN).

10

24. An ATM mobile terminal (MT) for setting up a secured
communication (WCC) to an ATM access node (AN) of a
wireless ATM communication network (WATM), comprising:

15

a) a setup means (MT-SET) for setting up (S2) a
wireless ATM radio communication connection (WCC)
to said ATM access node (AN) without performing
(ST2, ST3) an authentication information checking
procedure therebefore;

20

b) a secret communication key storage means (CK-MEM)
for storing a secret communication key (CK) used
by said ATM mobile terminal (MT) and said ATM
access node (AN) for performing wireless ATM
communications.

25

25. An ATM mobile terminal (MT) according to claim 24,
characterized in that
an authentication means (MT-AM) of said ATM mobile
terminal (MT) sends an authentication information
request message (AI-RQST; S3) to a network
authentication device (SSD) provided by said wireles
ATM communication network (WATM) or an interconnected
fixed network (FN).

35

26. An ATM mobile terminal (MT) according to claim 25,
characterized in that

- 5 an authentication information reception means (MT-RM)
receives said authentication information (AI) from
said network authentication device (SSD) in response
to said request message (AI-RQST).
- 10 27. An ATM mobile terminal (MT) according to claim 26,
characterized in that
said authentication means (MT-AM) transfers said
received authentication information (AI) to said ATM
access node (AN).
- 15 28. An ATM mobile terminal (MT) according to claim 25 and
26, *characterized in that*
said ATM mobile terminal (MT) comprises a timer (TMR)
and if after said sending of said authentication
20 information request message (AI-RQST) an
authentication information (AI) is not received from
said network authentication device (SSD), an interrupt
means (MT-IM) of said ATM mobile terminal (MT) closes
said setup wireless ATM radio communication connection
25 (WCC) between said mobile terminal (MT) and said ATM
access node (AN).
29. An ATM mobile terminal (MT) according to claim 25,
characterized in that
30 said ATM mobile terminal (MT) comprises an automatic
repetition means (MT-AUTO) for automatically repeating
a setup attempt after a predetermined time intervall.
30. An ATM mobile terminal (MT) according to claim 29,
35 *characterized in that*
said ATM mobile terminal (MT) comprises a counter (MT-
CNT) which counts the number of repetitive attempts to
setup a connection by said setup means (MT-SET),

- 5 wherein an inhibition means (MT-INHB) inhibits further
 setup requests after a predetermined number (N) of
 attempts.
- 10 31. An ATM mobile terminal (MT) according to claim 24,
 characterized by
 a secret key selection means (MT-SEL) for selecting a
 secret key (CK) used for the wireless ATM
 communication connection (WCC).
- 15 32. An ATM wireless communication network (WATM),
 comprising at least one ATM mobile terminal (MT)
 according to one or more of claims 24-31, at least one
 ATM access node (AN) according to one or more of
20 claims 15-23 and an exchange means (EX) for setting up
 ATM wireless radio communication connections (WCC)
 between said at least one mobile terminal (MT) and
 said at least one ATM access node (AN).
- 25 33. An ATM wireless communication network (WATM) according
 to claim 32, *characterized in that*
 to said wireless ATM radio communication network
 (WATM) is connected a non-ATM fixed network (FN)
 providing functions and services to a plurality of
 fixed network subscribers (SS), wherein said ATM
30 mobile terminal (MT) accesses said functions and
 services via said wireless ATM radio communication
 connection (WCC) setup between said ATM mobile
 terminal (MT) and said ATM access node (AN).
- 35 34. A method according to claim 4,
 characterized in that said authentication information
 (AI) is transferred back to said mobile terminal (MT)

38

5 through said setup secured communication connection
 (WCC).

35. A device according to claim 12,
 characterized in that said transmission means (TR)
10 transfers back said authentication information to said
 mobile terminal (MT) through said setup secured
 communication connection (WCC).

36. An access node (AN) according to claim 16,
15 characterized in that a transmission means (TR) of
 said access node (AN) transfers back said
 authentication information to said mobile terminal
 (MT) through said setup secured communication
 connection (WCC).

20

37. An ATM mobile terminal (MT) according to claim 26,
 characterized in that said authentication information
 reception means (MT-RM) receives said authentication
 information (AI) through said setup secured
25 communication connection (WCC) setup between said
 access node (AN) and said ATM mobile terminal (MT).

38. An ATM mobile terminal (MT) according to claim 27
 characterized in that said authentication means (MT-
30 AM) transfers said authentication information (AI)
 through said secured communication connection (WCC)
 setup between said access node (AN) and said ATM
 mobile terminal (MT) to said access node (AN).

1 / 6

Fig. 1a
PRIOR ART

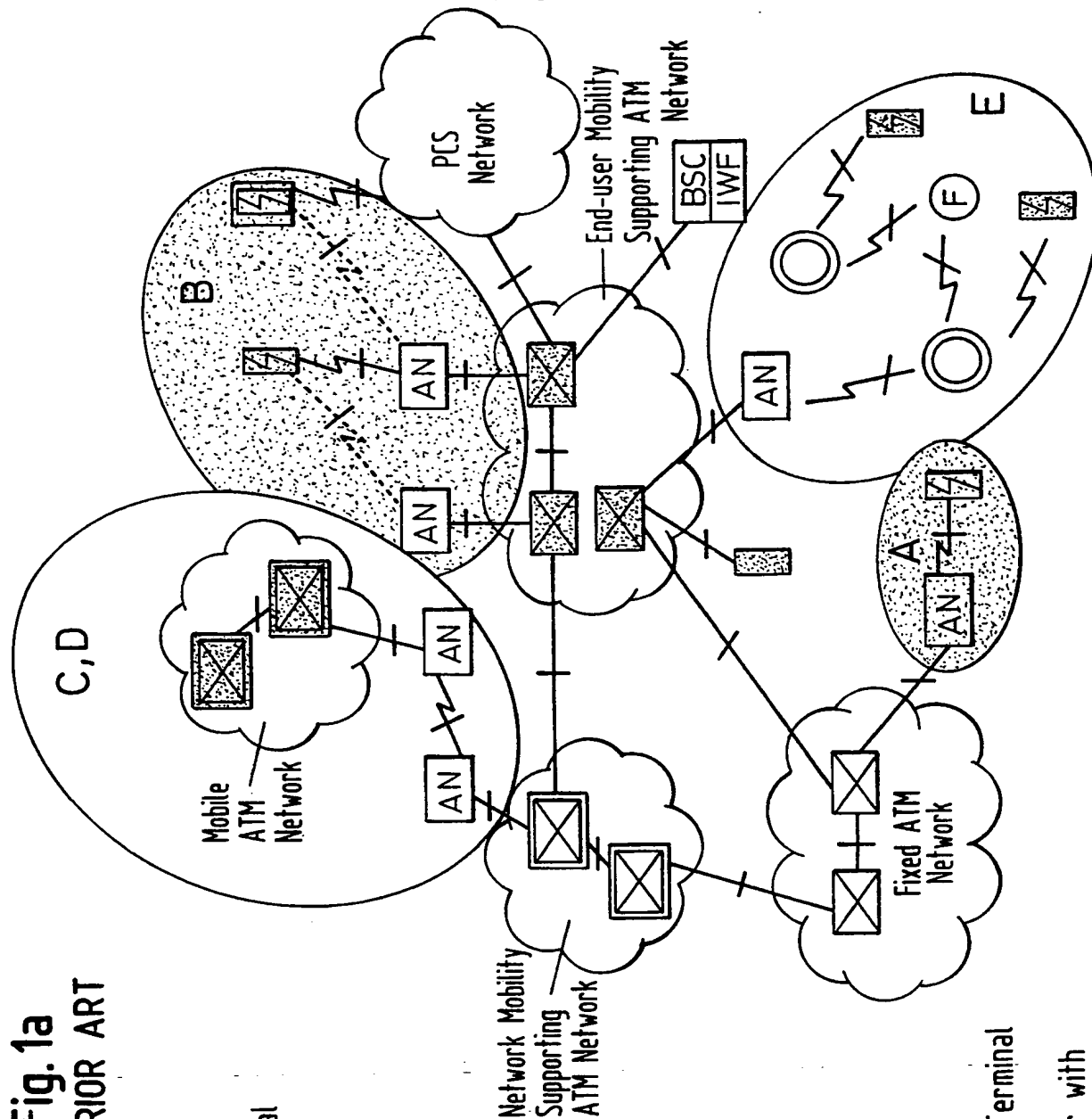
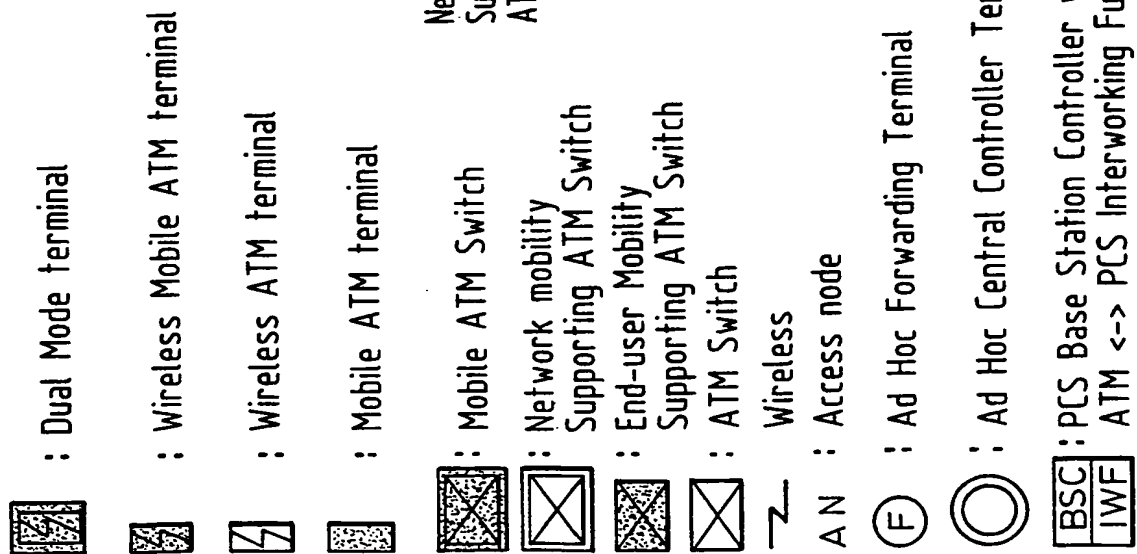


Fig. 1b
PRIOR ART

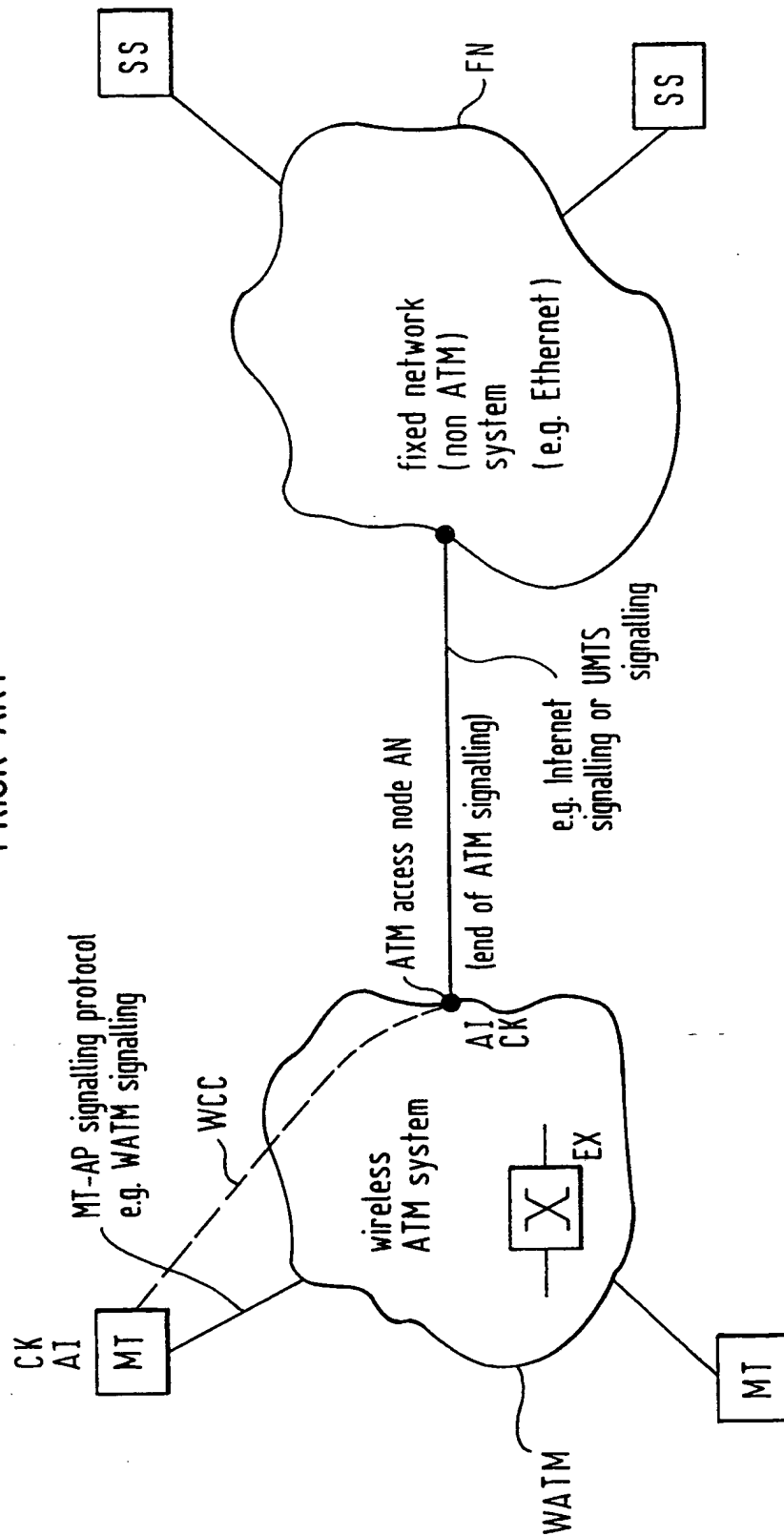
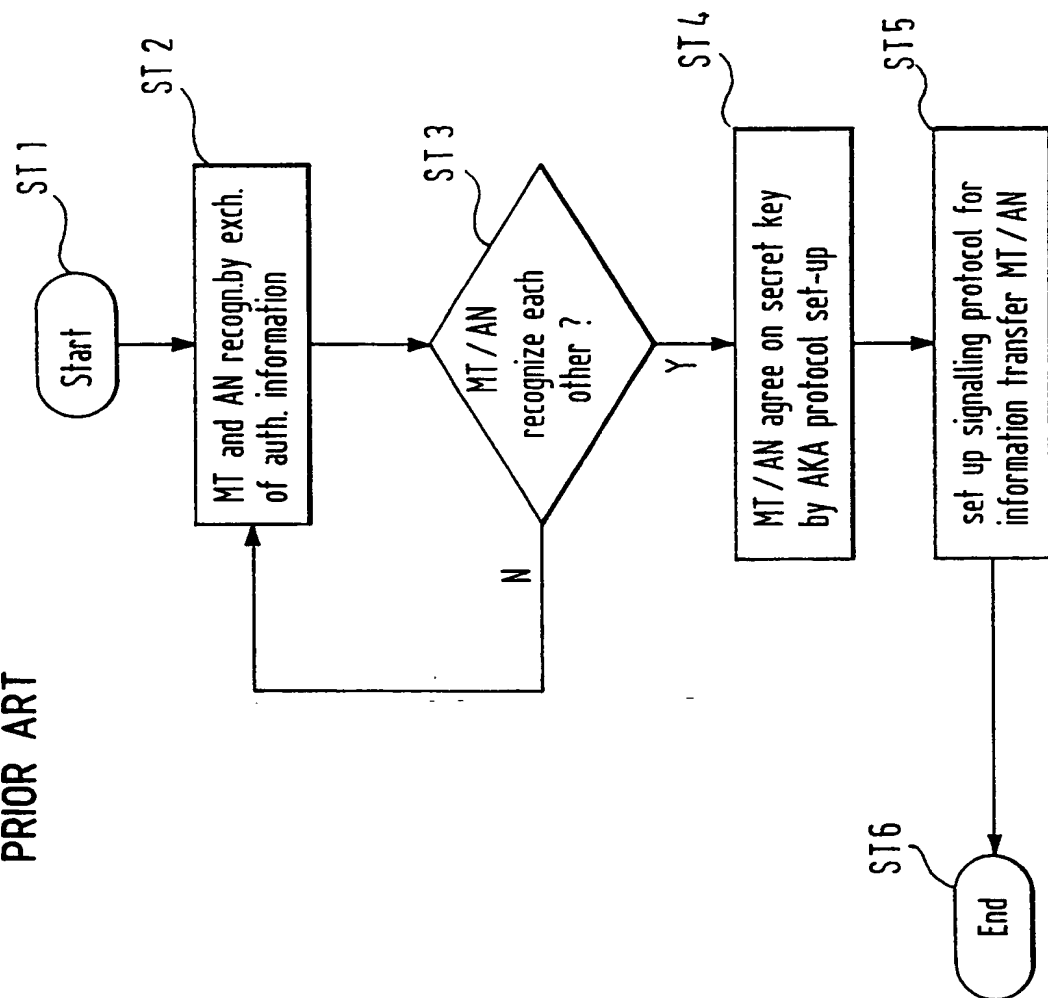
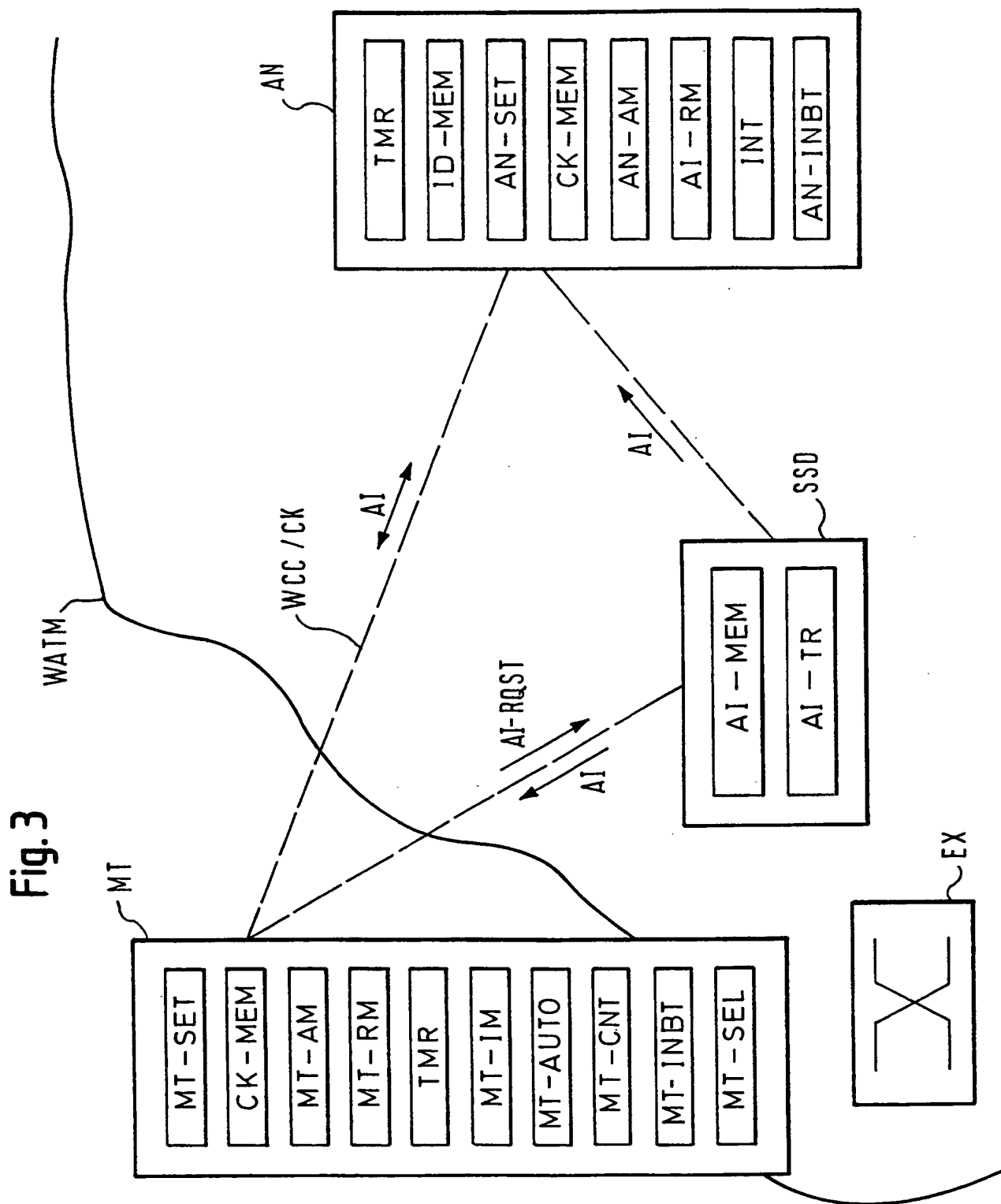


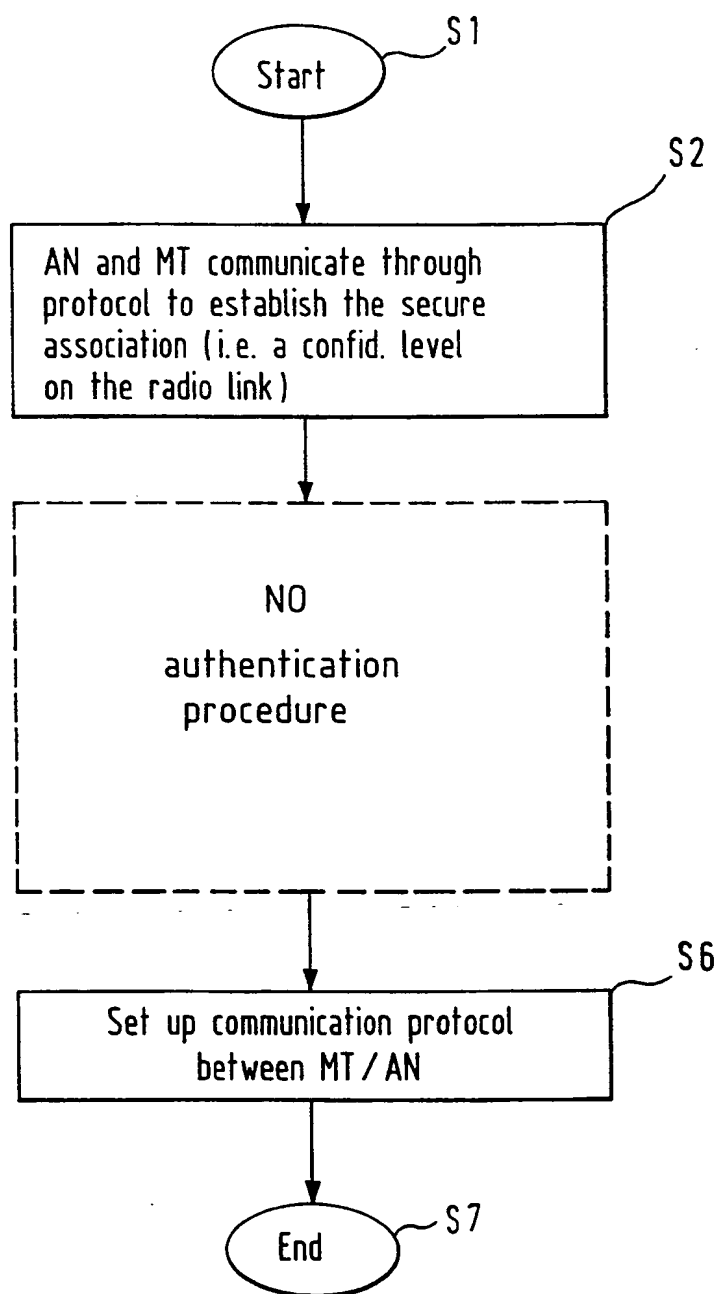
Fig. 2
PRIOR ART





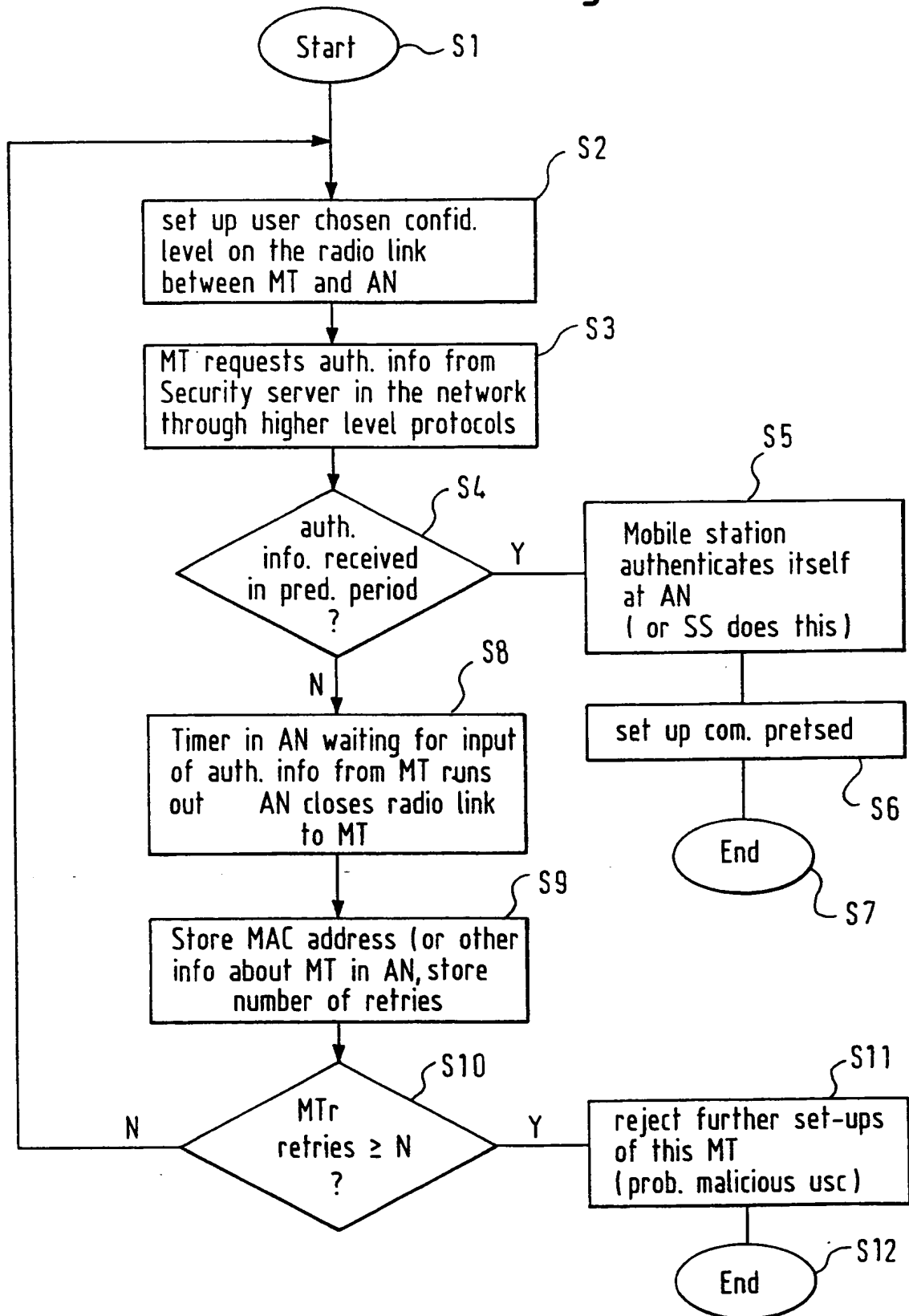
5 / 6

Fig. 4



6 / 6

Fig. 5



INTERNATIONAL SEARCH REPORT

Int. l. Application No

PCT/EP 99/01251

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04Q11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 813 346 A (ASCOM TECH AG) 17 December 1997 see column 3, line 10 - line 23; figure 4 see column 6, line 56 - column 7, line 27 ---	1-38
A	EP 0 800 298 A (MOTOROLA INC) 8 October 1997 see column 4, line 27 - column 5, line 52 ---	1-38
A	US 5 539 744 A (CHU HELEN ET AL) 23 July 1996 see column 17, line 23 - line 29 see column 30, line 23 - line 36 -----	1-38

☐

Further documents are listed in the continuation of box C.

☒

Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

10 June 1999

Date of mailing of the international search report

21/06/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Gregori, S

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 99/01251

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0813346 A	17-12-1997	WO 9739595 A	23-10-1997
EP 0800298 A	08-10-1997	US 5872523 A	16-02-1999
US 5539744 A	23-07-1996	NONE	